

REMARKS

Claims 1-11, 17-20 and 28-37 are pending. Claims 1-11, 17-20 and 28-37 are rejected. Claims 1, 17, 28, 30, 34 and 35 are amended.

This Response is filed in reply to the Final Office Action dated May 5, 2004. Applicant's silence with regard to any of the Examiner's rejections should not be construed as acquiescence to any of the rejections. The amendments to the claims are being made solely to expedite the prosecution of the above-identified application. Applicant reserves the option to further prosecute the same or similar claims in the instant or subsequent patent applications. Upon entry of the Amendment, claims 1-11, 17-20, and 28-37 are pending in the present application.

The Examiner rejected claims 1, 4, 5, 7-9, 11, 17, 18, 20, 34, 36 and 37 under 35 U.S.C. § 103(a) as being unpatentable over de Silva et al. (U.S. Patent No. 6,564,320).

The Examiner also rejected claims 2, 3, 6, 10, 19, 28-33, and 35 under 35 U.S.C. § 103(a) as being unpatentable over de Silva in view of Vaeth et al. (U.S. Patent No. 6,308,277).

Applicant traverses the Examiner's rejections and respectfully requests reconsideration in view of the amendments and remarks.

Applicant's independent claim 1 is directed to a method for certificate generation, which enables efficient revocation of the certificate. Among other things, Applicant's independent claim 1 includes a first node and a second node. The first node receives a request for issuing a certificate on behalf of a principal and forwards the request to the second node, in which the request includes a first identifier that identifies the first node. Subsequently, the second node generates a certificate that includes *the first identifier for the first node from whom the second node received the corresponding request for the certificate*. If the security of the first node is determined to be compromised, the certificates requested by the first node can be revoked by reference to certificates containing the first identifier.

Applicant agrees with the Examiner's statement that the patent to de Silva et al. "does not explicitly state that the certificate includes said first identifier" and that deSilva et al. mention that "all communications preferably occur over secure communication links". However, in the rejections of claim 1 and in the Examiner's response to Applicant's arguments, the Examiner contends that since all communications in the deSilva et al. patent preferably occur over secure communication links, one of ordinary skill in the art would be motivated to include the identifier of the certificate request in the generated certificate for more securely monitoring the generated certificates. Applicant respectfully disagrees.

In a first instance, deSilva et al. do not teach or suggest monitoring the certificates. Without first showing that deSilva teaches or suggests monitoring certificates, it follows that there can be no showing of a motivation to more securely monitor the certificates. Further, as described by deSilva et al. and as known in the art, secure communication links are used to safeguard sensitive information being transmitted over the links. In this regard, deSilva et al. suggest the use of "the SSL protocol where possible" (col. 12, lines 49 and 50).

The Secure Sockets Layer (SSL) protocol is commonly used for managing the security of a message transmission on the Internet. Managing the security of a message transmission between a first node forwarding a request for a certificate and a second node providing the certificate is unrelated to providing an identifier of the first node within the certificate. The SSL protocol provides for securely identifying the parties using the secure communication links. However, Applicant is unaware of any provisions in the SSL protocol, or other known protocols for secure communications links, for recognizing an identifier of the first node included in the certificate provided by the second node. Thus, the use of the SSL protocol for secure communication links, as mentioned by deSilva et al., is not seen to motivate one of skill in the art to include such an identifier in a certificate.

As described by Applicant, current systems and methods lack efficient means to revoke certificates issued at the request of untrustworthy registration authorities. Using current systems and methods, each certificate must be revoked individually and must be listed in and tested against a certificate revocation list to ascertain whether the specific

certificate is contained on the list. By providing a *first identifier* for a registration authority in the certificate, Applicant enables efficient identification and revocation of certificates associated with the identified registration authority.

The deSilva et al. patent does not address the problem of efficient revocation of certificates issued at the request of untrustworthy registration authorities. The deSilva et al. patent is directed to enabling a local hosting of digital certificate services, e.g., on local servers operated by affiliates of a certification authority (col. 2, lines 36-40). The digital certificate services related to revocation offered by deSilva et al. include Check Status, Verification, Revocation, and Replacement. Each of these services, which deSilva et al. put forth as a preferred embodiment, is directed to a single certificate, as provided by current systems and methods (col. 4, line 53 to col. 5, line 9). In the environment of the preferred embodiment described by deSilva et al., there is no recognition of a problem of inefficient revocation of certificates issued by untrustworthy registration authorities. Thus, deSilva et al. provide no teaching, suggestion and/or motivation to provide an additional identifier in the certificate for the registration authority requesting the certificate.

Based on the above, Applicant respectfully requests that the Examiner reconsider the conclusion that the use of secure communication links, as described by deSilva et al., teaches or suggests monitoring certificates. Further, Applicant respectfully requests that the Examiner reconsider the conclusions that the use of secure communication links would motivate those of ordinary skill in the art to more securely monitor certificates and that those of ordinary skill in the art would have found it obvious to modify the certificates of de Silva et al. to include Applicant's claimed *first identifier* to provide more secure monitoring of certificates.

In view of the above remarks, Applicant respectfully suggests that independent claim 1 is in condition for allowance, and allowance is requested. Applicant's independent claims 17, 28, 30, and 34 are directed, respectively, to certification authorities, computer program products, computer data signals, and apparatuses, each including features similar to independent method claim 1. Applicant respectfully suggests that independent claims 17,

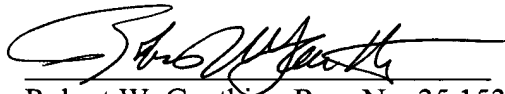
28, 30, and 34 are therefore allowable for the reasons provided with respect to independent claim 1. Claims 2-11, 18-20, 29, 31-33, and 35-37 depend from independent claims 17, 28, 30, and 34 and are allowable, at least by dependency.

CONCLUSION

On the basis of the foregoing Amendment and Remarks, this application is in condition for allowance. Accordingly, Applicant requests allowance. Applicant invites the Examiner to contact the Applicant's undersigned Attorney if any issues are deemed to remain prior to allowance.

Respectfully submitted,

Date: July 2, 2004
Customer No: 25181
Patent Group
Foley Hoag, LLP
155 Seaport Blvd.
Boston, MA 02210-2600


Robert W. Gauthier, Reg. No. 35,153
Attorney for Applicants
Tel. No. (617) 832-1175
Fax. No. (617) 832-7000